UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/652,157	08/31/2000	Motoji Oomori	04329.2371	2617

22852 7590 03/08/2004

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
1300 I STREET, NW
WASHINGTON, DC 20005

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 03/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/652,157	OOMORI ET AL.	
	Examiner	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 August 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *27-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *27-30,32-39 and 41-46* is/are rejected.

7)☒ Claim(s) *31 and 40* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 August 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4,6,7,8,10*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 28-46 are pending.

2. The IDS of 12/1/00 (#4), 7/29/02 (#6), 11/7/02 (#7), 11/13/02 (#8) & 3/12/03 (#10) have been received and considered.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 27, 28, 30, 35-37 & 39 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent 5,442,705 to Miyano.

Regarding claims 27, 35 & 36, Miyano discloses a plurality of key transform devices/circuits (col. 1 lines 64-68 & col. 2 lines 1-28), an exclusive-OR element calculating an exclusive-OR (Fig. 2 #16) of a constant/R (Fig. 2) determined for each of the key devices/rounds and a first key/Kn obtained from the input key/Kn (Fig. 1), a transform unit/s-box nonlinearly transforming (Fig. 2 S1-S8) the output from the exclusive-OR element (Fig. 2 #16), an expansion unit/E1 and an expansion key calculation unit/EX-An calculating the expansion key/(K1-Kn) based on an output from the expansion unit/E1 and a second key/Kn obtained from the input key/Kn (Fig. 1 & Fig. 2, col. 2 lines 45-68, col. 3, col. 4 & col. 5 lines 1-28).

Regarding claims 28 & 37, Miyano discloses a rotation unit/key scheduling section for shifting the input key to at least or most significant bit and inputting the shifted key to the key transform device of a next stage/round (col. 2, lines 65-68 & col. 3 lines 1-44).

Regarding claims 30 & 39, Miyano discloses shifting a predetermined number of bits (Table 2).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim 29, 32, 38 & 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Miyano.

Regarding claims 29 & 38, Miyano discloses a block ciphering arrangement, but does not disclose shifting by an amount relatively prime to the number of output bits of the nonlinear transform unit. However, it was known, by one of ordinary skill in the art of cryptography, at the time the invention was made, that the shifting of bits by numbers not relatively prime would negatively result in repetitions/patterns. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to shift by an amount relatively prime to the number of bits output by the nonlinear transform unit. One of ordinary skill in the art would have been motivated to perform such a modification to eliminate detrimental patterns and repetitions, as was known to do so.

Regarding claims 32 & 41, Miyano does not explicitly disclose the expansion key calculation unit/EX-An performing addition of the output of the expansion unit E1 and the second key with carry up. However, the expansion key calculation unit/EX-An (Fig. 1) is an XOR function, which is a modulo-2 addition. Further, while Miyano does not disclose a carry up addition, it was commonly known in the art of digital circuitry to perform addition with carry up, at the time the invention was made. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to perform addition with carry up. One of ordinary skill in the art would have been motivated to perform such a modification because it was commonly known in the art to do so.

7. Claims 33, 42 & 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Miyano, as applied to claims 28 & 36, in view of U.S. Patent 5,787,179 to Ogawa et al. (Ogawa). Miyano discloses a system, as described above, but lacks including the key expansion circuit in an encryption circuit/data randomization unit. However, Ogawa teaches that it is known to include a random number generator/key expansion circuit in an encryption device to generate random numbers based on a key signal (col. 6 lines 20-31). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the key expansion capabilities of the Miyano invention with the encryption circuit of Ogawa. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of generating random numbers based on a key signal, as taught by Ogawa (col. 6 lines 20-31).

8. Claims 44 & 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Miyano in view of "Random Number Generators for Parallel Applications" by Srinivasan. Miyano discloses a system, as described above, but lacks the circuits specifically being "parallel". However, Srinivasan teaches that to achieve greater speeds in random number generators, it is known to parallelize components (page 9 §*Parallelization* ¶1-2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to parallelize the key transform devices. One of ordinary skill in the art would have been motivated to perform such a modification to achieve greater speeds, as taught by Srinivasan (page 9 §*Parallelization* ¶1-2).

9. Claims 34 & 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Miyano in view of Ogawa, as applied to claim 33, in further view of "Applied Cryptography, Second Edition" by Schneier. Miyano discloses a system, as modified above, but lacks explicit disclosure of common substitution elements. However, Schneier teaches that FEAL, which requires fewer rounds than DES (page 308 §13.4 ¶1), implements a block-ciphering algorithm and key generator that use identical substitution elements (Figs. 13.3, 13.4, 13.5 & 13.6 on pages 308-310). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the same substitution tables for the nonlinear transform and the data randomization unit. One of ordinary skill in the art would have been motivated to perform such a modification as it was known to do so in block-ciphering algorithms such as FEAL that uses fewer rounds than DES (page 308 §13.4 ¶1), as taught by Schneier.

Allowable Subject Matter

10. Claims 31 & 40 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

11. The following is a statement of reasons for the indication of allowable subject matter:

a. Regarding claims 31 & 40, the prior art relied upon fails to teach or suggest shifting the output from the nonlinear transform unit by the specific number of bits calculated by the procedures in the claim (1/2 the number of bits of the output or by the number of bits obtained by adding an integer multiple of the number of bits of the output to the half number of bits).

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patents 6,570,989, 5,317,638, 6,606,385, 6,246,768, 6,292,896, 6,683,956 are cited for using s-boxes/substitution elements, XOR elements and data expansion for key generation and encryption/decryption in a similar fashion to that of the claimed invention.

The non-patent references by Aiello, Keliher, Han, Seo & Lim are cited for using similar structures as the claimed invention for key generation and encryption/decryption and also for discussing hardware implementations of key generators and

encryption/decrypt units. The Aiello reference specifically discloses the use of block-ciphering methods to generate pseudo-random numbers.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")
Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

MJS
February 27, 2004

NORMAN M. WRIGHT
PRIMARY EXAMINER